NOVEMBER 2025

Cybersecurity Program Policy

NORTHEAST MISSOURI RURAL TELEPHONE COMPANY | GREEN CITY, MISSOURI

Table of Contents

1 Purpose

NEMR is dependent on interconnected technologies to provide services to its customers. Disruption, destruction, and unauthorized access to these technologies undermine telecommunication operations. This policy has been adapted to provide strategies, training, and intelligent responses to these cybersecurity threats.

The Cybersecurity Program establishes formal procedures for training, monitoring, and responding to cyber threats. Cyber threats can strike at any time and come in many forms. NEMR strives to implement procedures for obtaining, monitoring, assessing, and responding to evolving threats and vulnerability information.

2 Cybersecurity Training & Awareness

2.1 Management Responsibilities

The NEMR Board is responsible for overseeing the development, implementation, and maintenance of the institution's cybersecurity program and holding senior management accountable. The board should reasonably understand the business case for cybersecurity and the business implications of:

- Cybersecurity risks
- Provide management with direction surrounding cybersecurity
- Approve cybersecurity plans, policies, and programs
- Review assessments of the cybersecurity program's effectiveness
- When appropriate, discuss management's recommendations for corrective actions

The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the cybersecurity program. The board should approve the institution's written cybersecurity program; affirm responsibilities for the development, implementation, and maintenance of the program; and review any changes to the plan.

Management should provide a report to the board of any incidents that occur. The report should include any security breaches, violations of law or regulations, and management's responses to such incidents.

When providing reports on cybersecurity, management should include:

- The results of management assessments, reviews, and pertinent notes or recommendations.
- Internal and external audit activity related to information security.
- Third-party reviews of the cybersecurity program and cybersecurity measures.
- Other internal or external reviews that are designed to assess the adequacy of the cybersecurity program, processes, policies, and controls.

Management also should do the following:

- Implement the board-approved cybersecurity program.
- Establish appropriate policies, standards, and procedures to support the cybersecurity program.
- Participate in assessing the effect of security threats or incidents on the institution and its lines of business and processes.
- Delineate clear lines of responsibility and communicate accountability for cybersecurity

Management is also responsible for providing adequate support to IT personnel when executing the Incident Response Policy.

2.2 Employee Responsibilities

The protection of IT systems is the responsibility of all employees and management of NEMR. IT Security begins with the employees of NEMR that operate its equipment daily. Management and employees must support IT personnel by understanding IT risks and vulnerabilities and report issues to proper personnel. IT personnel must identify abnormalities and conduct formal investigations. Every employee has unique responsibilities at NEMR and each is designated to a group that is defined by the organization's layout.

Employee roles include monitoring the equipment they utilize for anomalies. An employee should understand the normal operation of their equipment and possess the ability to report problems. When reporting problems to IT personnel, employees should be able to reasonably respond to the guidance given. Employees will follow the procedures defined by policies while working to create a security-based culture at NEMR.

Management will provide an annual agreement to include an Acceptable Use Policy and Non-Disclosure Agreement to employees that verify they have read and understand the cybersecurity policies. Employees should be committed to integrating the program into the institution's lines of business, support functions, and third-party management programs. This will be done by an acknowledgment that the employees understand, are responsible for and accountable to the information presented through the IT training and cybersecurity policy.

2.2.1 Email & Internet Acceptable Use

Employees are to understand that email, internet, and access to all other communication platforms is given solely for businesses purposes. Unacceptable usage of these assets includes but is not limited to:

Viewing, storing, or exchanging content that can be interpreted as:

- Harassment, discriminatory, offensive, or threatening comments
- Adult content, and abusive material
- Any illegal activities – blackmail, copyright infringement, extortion, etc.

Employees are prohibited from abusing company resources to disrupt the production of others whether this is another employee or individuals outside of the institution. Employees are forbidden from downloading and installing any software, programs, or online resources without the approval of a supervisor or the IT department. Employees must understand that all data they transmit through email, internet, and other communications platforms are their responsibility and that they represent NEMR while utilizing these resources.

Furthermore, NEMR reserves the right to monitor, access, & seize any company issued device any given time without warning as these assets are property of the institution. Employees should have no expectations of privacy regarding the activities conducted and data stored on their devices. Failure to comply with standards listed in this policy will result in disciplinary action up to and including termination. If employees have any questions regarding this policy they should be directed towards their immediate supervisor.

2.3 Social Media Policy

In the modern-day social media is a tool which can be utilized to build business relationships and enhance marketing strategies. However, if used improperly social media can have negative consequences for the individual employee and the business. NEMR has created this policy to better protect the online presence of the institution and its employees. This policy defines social media as any form of communication over the internet. Currently NEMR has a Website, Facebook page, Instagram, YouTube, Tik Tok, LinkedIn and WhatsApp account.

2.3.1 Employee Guidelines to Social Media

Like the Acceptable Use Policy, employees must understand that whether they post during or outside of business hours they represent NEMR, and the information they submit online can be taken out of context. NEMR does find it perfectly acceptable for employees to share positive news and information regarding the organization if it is depicted in a positive manner and does not disclose any confidential information. Employees should use caution and good judgement before posting and heed the following guidelines:

- Avoid sharing sensitive information regarding NEMR, a fellow employee, a client, or other business relationships.
- Maintain a respectful presence. Do not post anything that may be seen as abusive, threatening, discriminatory, etc.
- Be cautious when posting pictures or your location, especially those that contain company assets. Before posting pictures containing other individuals, get their permission before uploading them online.
- Do not act like a NEMR spokesperson without company approval.
- If in doubt about whether information is confidential or not, treat it as confidential.

2.4 Awareness & Education Program

The cornerstones of cybersecurity training are people, processes, and technology. Informational security training is used to reinforce the knowledge of the processes around the use of technology. All personnel must be aware of information security threats that affect them in their day-to-day business operations. Security training will have a formal process for educating employees of each group defined by their roles and responsibilities. Information in the training will include but is not limited to:

- Information systems and cybersecurity program
- Social engineering tactics including phishing and vishing
- Third-party personnel processes
- Malware, viruses, and ransomware
- Email Safety and Spam

This training will be conducted at least monthly through webinars, in-person, or done as part of another training program. Training shall be a mandatory process and will be held for all staff and board members. Additionally, all

newly hired staff members or any unable to attend the alternative training courses will have separate training courses to ensure full company coverage.

Awareness testing will be conducted to ensure NEMR employees understand the threats they come in contact with as well as the adherence to the NEMR policies. NEMR will test employees on what they have learned to ensure they understand their responsibilities in the security process. The testing of employees will be done with proven tools and methods that will include social engineering as well as access control and awareness testing. This can entail the use of phishing either onsite or by remote means and can include impersonation through calls, emails and text messages. NEMR IT administrators and management are responsible for the training, testing, and upkeep of any testing standards of its employees. The IT Manager is responsible for conducting monthly awareness testing and trainings and will maintain logged activity of all users.

2.5 Employee Remote Work Policy

Please refer to separate Remote Work Policy.

3 Cybersecurity General Policies

3.1 Onboarding & Offboarding Policy

During both the onboarding and offboarding process internal staff will follow the guidelines in this policy as well as the checklists labeled in the **form appendix** of this document. The onboarding process will consist of granting minimum access to the network for business purposes, conducting the human resources requirements, and initial security training. When an employee is terminated or resigns, they will surrender all company devices and credentials. Any ongoing projects will be reviewed with the supervisor and transferred to the appropriate parties. Further detail is outlined in the onboarding & offboarding forms.

3.2 Segregation of Duties

Dual controls and segregation of duties are implemented on system administrators of the network. Each administrator has two separate accounts granted to them. The first account will be a standard user for everyday business tasks. The second account will be administrator-level privileges to be used only for administration work. Each account is not allowed to have the same password. Furthermore, administrative duties are assigned to ensure at least two employees will have access to critical assets. This ensures that in the event one administrative employee is unavailable business operations may continue efficiently.

3.3 Decommission of Devices

When a device has been identified for its end of life, approximately 5 years for employee machines management will track this device and plan the sunsetting of any end-of-life devices. NEMR utilizes a Software Deployment Appliance for its inventory tracking. This tracking system will be referred against the IT asset list and reviewed at least on an annual basis. When a device containing sensitive information is removed from the network, only when a stable, testing replacement is in place can the process of dismantling and disposing of taking place. The process of removing its hard drives will be conducted and any other parts that may contain sensitive data. Each hard drive will be rendered unrecoverable according to NIST standards (special publication 800-88, Revisions 1 on guidelines for media sanitation). This is being done to protect NEMR and its private data and clients.

3.4 Network Controls

Network access controls will be provided to employees by domain permissions. Permissions will be granted based on the job description and will only allow authorized individuals access to customer or proprietary information. At no time will employees disclose sensitive information to unauthorized individuals who may seek to obtain this information for malicious reasons.

- Network access and system access will require username and password use
- Network passwords will be at least 8-12 characters in length, lowercase, upper case, and character rotation of re-using password 3 times along with password change every 90 days.
- Access levels will be set based on job functionality and be reviewed periodically by the IT and Network Manager.
- Access will immediately be terminated after an employee leaves the company

4 Data Encryption

Protected private or confidential information is only stored by NEMR when there is a required business need. If sensitive information is required to be stored by NEMR in any form, it is done so in a secure manner designed to prevent potential threats even in the event of a breach. Confidential data at rest or in transit should be encrypted using strong current cryptography. Encryption is used to secure data, transmission, and communications particularly authentication credentials and sensitive data. Encryption is used as a control to protect data and provide confidentiality, integrity, and availability. The system administrators are responsible for maintaining and enforcing NEMR data security policies, with the intent of minimizing risk. PII and backups are encrypted through Azure and Wasabi.

4.1 Data Transmission

Data transmissions of customer or sensitive information are restricted to methods that provide encryption or protection specifically authorized and approved by the system administrators. Protected data transmitted outside of the NEMR environment is only sent over encrypted channels, such as SSL/TLS, SSH, Virtual Private Networks (VPNs), or dedicated lines. Transmission of protected information is only done as required by business, legal, or regulatory obligations.

4.2 Data Storage and Security

Data storage is always kept to a minimum. Sensitive customer authentication data is not stored unless absolutely necessary to fulfill a business or legal obligations, including full track magnetic stripe data, card verification code, or personal identification numbers (PINs). All required customer information is kept only as long as required to fulfill business, legal, and regulatory requirements. Documents and media containing customer information are stored in locked desks, storage containers, or secure areas always.

Retained confidential company and customer information need to be periodically disposed of. NEMR has procedures in place to destroy customer information that is no longer necessary, up to and including:

- Shredding of documentation
- Overwriting of media
- Formatting/Erasing
- Physical destruction of documentation and media

A yearly review is conducted to ensure all confidential data is being properly disposed of after all business, legal, and regulatory obligations are met.

4.3 Encryption Keys

Stored customer information is always encrypted inside Innovative Systems Elation rendering confidential information completely unreadable. Access to a customer or critical data, including encryption keys, is restricted to authorized personnel and is only granted as necessary by the IT Manager and/or Network Manager. Any storage of encryption keys is limited to as few locations as possible.

Encryption key management processes are derived from the National Institute of Standards and Technology (NIST) standards to be as cryptographically secure as possible. Management processes and procedures include the following:

- Strong key generation, preferably at minimum 256-bits where possible
- Secure key distribution
- Secure key storage
- Changing of keys with expired crypto periods
- Removal of weak or compromised keys
- Prevention of unauthorized key substitutions
- Documentation of key custodians

5 Confidentiality and Privacy Policy

NEMR owns certain confidential information crucial to its business, including, but not limited to, operation, corporate records, business or financial affairs, know-how, processes, marketing plans, contracts, techniques, products, services, forms, research, and development, and business plans. NEMR also owns confidential information about its existing and prospective customers, including their identities, contact information, customer needs, correspondence, customer records, referrals, new business records, market data, financial information, etc. These are all defined as "trade secrets" as that term is used in state statutes. NEMR and its employees have a responsibility to protect any and all confidential or proprietary information and trade secrets against harmful or unauthorized distribution.

All employees, both as a condition of employment and after employment, must preserve NEMR's trade secrets, proprietary and confidential information, and may not use any of this information to benefit themselves or any business or person other than NEMR. If you are uncertain whether the information you wish to impart is confidential or a trade secret, check with a member of management before providing the information. As a rule of thumb, if the information cannot be commonly accessed by the general public through public means, do not impart the information without prior approval from the General Manager.

Confidential information also includes information considered gossip or hearsay to a third party about any of NEMR's customers gained as a result of your employment with NEMR. Creating, sharing, distributing, or disseminating information to others outside NEMR that is received as a result of your employment is strictly prohibited and considered a violation of this policy. Failure to follow this policy may result in discipline up to and including termination.

6 Cybersecurity Monitoring

6.1 Internal Networking Standards

Internal resources include intrusion prevention systems, intrusion detection systems, firewall logs, server event logs, antivirus alerts. Once the institution understands the baseline of its network, monitoring systems can be implemented and tuned to provide alerts to activity that is outside of the baseline and requires additional analysis by trained technical staff. Data Security will be classified into three categories of sensitive data:

1. Public Information: This includes all information that can be freely disclosed without violating an individual's rights of privacy. This information must not expose NEMR to any adverse risk when being disclosed. Examples are public annual reports, press releases, and geolocation information.
2. Sensitive Internal Data: Includes all information that can only be disclosed to personnel at NEMR. Exceptions are made to regulators and all people covered by a signed non-disclosure agreement. Examples are internal email directory, policies, employee handbook, and organizational chart.
3. Confidential Information: Includes all information pertaining to customer information. This information can include but is not limited to name, address, telephone number, social security number, driver's license, account number, credit or debit card numbers, or passwords. Unauthorized disclosure or destruction may result in financial loss, damage to NEMR's reputation and business, and potential legal action. Examples are Username, Passwords, Account numbers, credit reports, and financial plans.

6.2 Equipment Hardening Guidelines

It is common when purchasing new devices such as workstations & networking equipment that these devices are by default configured with unnecessary functions and features that may pose additional risk when implemented into NEMR's IT infrastructure. Due to this fact, NEMR requires that all new devices undergo a standard hardening process to ensure all irrelevant settings are disabled and that modern security controls are properly configured. The IT Manager and/or Network Manager will coordinate with the vendor's support representatives to establish and confirm best security practices on the device. After a new device has been successfully added to the network NEMR will conduct vulnerability scans to ensure no known vulnerabilities have been disregarded.

6.3 Device Patching Standards

Inadequate patching of software exposes devices to significant risk. Software vulnerabilities can cause systems to be unavailable, create security weaknesses, or allow the compromise of critical systems & data. Malicious software is known to use known vulnerabilities in their code. Limiting the time after a vendor has released a patch for these fixes is critical to daily operations.

NEMR administrators are responsible for managing the patching of devices on the network.

Software Deployment Appliance is used to monitor NEMR's network. This software is used for an internal device list. This will be referenced against for responsibilities of each device on the network. Monthly or as needed this list will be reviewed for new patches to be applied.

Windows Server Update Services (WSUS) should be utilized, when possible, to provide features, manage and distribute updates through a management console. A WSUS server can also be the update source for other WSUS

servers within the organization. The WSUS server that acts as an update source is called an upstream server that processes and serves updates to the clients on the network.

Currently, Automated Endpoint Management Platform is utilized on all employee devices. This system defends against malware using signature-based anti-virus. Malware is detected based on the digital fingerprint of its files. The anti-virus will detect and stop the malware before it is run on the device. With only using predefined signatures this software is critical to update for all devices. Stopping malware from entering the network will provide better longevity in the network.

6.4 3rd Party Due Diligence

Due to resource restrictions or other means, third parties may be granted access to the network. Before access is granted, NEMR will evaluate each vendor and its risk to the organization. The board and management are ultimately responsible for overseeing these actions are conducted and approved.

1. Appropriate controls and data handling of NEMR's network is in place.
2. Ensure Non-Disclosure Agreements are in place. Confirming safeguards of NEMR's network & its customers.
3. Annually review each vendor and its risk to NEMR. During this monitoring, NEMR can request further information from third parties for review. Such as controls in place, security audits, and service agreements.
4. Management will evaluate the quality of service, control environment, and financial condition of the third parties providing NEMR with critical IT services.
5. Assessing whether each third-party relationship supports NEMR's overall objectives and strategic plans.
6. Evaluating prospective third-party providers based on the scope and importance of the services they provide.
7. Tailoring NEMR's third-party management program based on an initial and ongoing risk assessment of the NEMR's third parties and the services they provide.

6.5 Physical Security

Physical security and network security are linked due to the nature of networking systems and physical devices. Physical security should stop non-authenticated parties from accessing NEMR's computing devices & sensitive customer data locations. Throughout NEMR's buildings cameras are implemented and recorded. External doors are secured with pad codes, key locks, and RFID key fobs.

NEMR restricts access to its building past the lobby area. Authorized third parties will be allowed into server rooms and off-limits parts of the buildings only while escorted with IT staff or management. Storage rooms are restricted to technicians and required officer personnel. These storage rooms will be locked at all times.

All external third parties are required to sign in & out at each location on a sign-in sheet. Employees must be present while third parties sign in and out at the front desk. Scheduled visits are requested by all third parties. Additionally, lists of onsite visits will be kept for a minimum of one month. This list will be used in case of an emergency or incident. Allowing for review of all parties that entered the building during that time in question.

6.6 Physical/Removable Media Policy

In addition to physical security, NEMR recognizes the dangers of unwarranted removable media such as USB sticks, CD's, etc. as they can be loaded with malicious content that could potentially spread throughout the network. Due to this fact NEMR forbids employees from inserting any sort of removable media into their devices, unless prior approval is given by a supervisor or the IT Team. To protect against malicious threats all workstations have Secure-IT installed to automatically scan inserted physical media and block its contents if deemed unsafe.

6.7 Risk Assessment

The process of understanding and defining risk to a company is vital in the growth and understanding of its risk appetite. NEMR on an annual basis will fill out and confirm the risk that is possessed to the company along with all mitigating controls and technology.

6.8 Mission Critical Assets

With the assistance of the Risk Assessment NEMR has identified all devices, assets, and business functions deemed crucial to upkeeping business operations. These assets have been marked in the Risk Assessment and will be prioritized for preservation and recovery in the event the incident response plan is initiated.

7 Incident Response Plan

7.1 Purpose

The documented Incident Response Plan (IRP) process includes four phases: Preparation, Identification, Protect & Recovery, and Post-Incident Activity. Incident Response is the process of planning, documenting, and communicating procedures to react to any threat that endangers the confidentiality, integrity, and availability of an organization's information and information systems. Incident Response has become necessary because attacks frequently cause the compromise of personal and business data. The following benefits are a result of having an effective Incident Response capability:

- Respond to incidents systematically to prevent indecision during an incident
- Recover quickly and efficiently from security incidents, in turn minimizing loss or theft of information, and disruption of services
- Utilize information gained during Incident Response to better prepare for future incidents and provide stronger protection for systems and data
- Dealing properly with legal issues that may arise during incidents

When a cyber security incident occurs, timely and thorough action to manage the impact of the incident is critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals are:

1. Preserve and protect the confidentiality of constituent, customer, and employee information and ensure the integrity and availability of NEMR systems, networks, and related data.
2. Help NEMR personnel recover their business process after a computer or network security incident or other type of data breach.
3. Provide a consistent response strategy to system and network threats that put NEMR data and systems at risk.
4. Develop and activate a communications plan including initial reporting of the incident as well as ongoing communications, as necessary.
5. Address cyber related legal issues.
6. Coordinate efforts with external Computer Incident Response Teams and law enforcement.
7. Minimize NEMR's reputational risk.

7.2 Preparation

Preparation is not only establishing an Incident Response capability, so the organization is ready to respond to incidents, but also preventing incidents by ensuring systems, networks, and applications are sufficiently secure. The Incident Response team's expertise should be valuable in establishing recommendations for securing systems. The Response Plan will be represented by a core set of doctrines, concepts, and processes that allow for effective responses:

- Identification: Establishment of appropriate escalation procedures to address varying alerts or incidents. Using the combination of planning, protocols, equipment testing, and training.
- Protect: Management will monitor the incident and relay pertinent information to authorities, employees, and third parties. NEMR will work to protect all affected systems and remove the threat.

- Response: Management will be designed to allow the Incident Response Plan to enable effective, efficient responses to the incident. The use of resources is crucial to allow for the success of the Incident Response Team.
- Recover: NEMR will use available resources to bring all affected systems back to a normalized state. Management will also document the incident during this phase.

Cyber incident response management is an on-going process with a cyclical pattern. The specific incident response processes include ensuring that systems, networks, applications, and data handling processes are sufficiently secure, and employee awareness training is in place. Exercises, phishing tests, and distributing literature are conducted periodically throughout the company. Examples of Questions that should be asked are but not limited to:

a. Has everyone been trained in security policies?
b. Have our security policies and incident response plan been approved by appropriate management?
c. Does the CIRT know their roles and the required notifications to make?
d. Have all CIRT members participated in mock drills?

An IRP accomplishes these objectives by creating an Incident Response Team (IRT), determining roles and responsibilities within and outside of the organization, defining and classifying levels of threat, developing responsive strategies accordingly, and performing regular tests and maintenance. These requirements are addressed in the following sections.

Team Role	Personnel	Contact Information
General Manager	Michele Gillespie	660.874.4111
Information Sec. Officer	Jason Hill/Jerry Hamilton	660.874.4111
Information Sec. Analyst	Jason Hill/Vantage Point	660.874.4111

General Manager - <Responsible for contacting outside media and making a public statement in the event of a cyber-attack.>

Information Security Officer – <Responsible for contacting third-party vendors affected by the attack, contacting forensic services provided through NEMR's cybersecurity insurance, and protecting/recovery critical systems and services.>

Information Security Analyst - <Responsible for reviewing firewall logs for initial means of compromise and assisting the ISO in protecting critical systems.>

7.3 Identification

When responding to an incident the IRT must first identify all physical and software access points that are affected. After determining the scope of affected systems, NEMR will respond according to the level of the incident. To facilitate the appropriate allocation of resources to incidents, an event classification hierarchy must be referenced in the IRP according to the following threat/event classifications:

1. High – All events that can cause significant damage or loss of property. It could possibly have significant repercussions financial and reputationally to NEMR. Examples:
    - Denial of Service or System Failure
    - System Compromise
    - Stolen or lost media of customer data
2. Medium – These events could possibly cause damage or loss of property. It may impact daily operations. Examples:
    - Unauthorized access to information systems
    - Single computer virus
3. Low – Events of this nature cause inconvenience and little cost associated with recovery. This can be handled internally with no material impact. Examples:
    - Minor system crashes
    - Minor system malfunctions

The Detection & Analysis phase begins with the identification of a potential computer security incident. The next step is the initial response which includes performing an initial investigation, recording basic details surrounding the incident, assembling the IRT, and notifying individuals who are required to know about the incident. Next is the formulation of a response strategy based on the results of all the known facts. The strategy will determine the best response and must obtain management approval. The Analysis component of this phase involves the information gathering techniques used in the initial response as well as the thorough collection of data and

reporting performed throughout the entire response including the next phase, Containment Eradication & Recovery.

7.4 Protect & Recovery

Containment Eradication & Recovery is the phase of the Incident Response Life Cycle that encompasses the actual performance of the agreed-upon Incident Response strategy. The course of action performed within this phase depends on numerous variables. It empowers staff to execute action determined by the Incident Response Team. Staff will work to recover any lost or exposed information. NEMR will work to restore systems back to their original state and protect them from the incident. The following sections will outline NEMR's response to specific security events.

7.4.1 Data Breach

Data Breaches can occur any time, the biggest concerns during a data breach are finding out the extent of the breach and stop it and future attacks.

1. Investigate the breach to determine the extent of the incident, start with the discovery of the incident through the next steps to be taken from there.
2. Determine roles and assess the next steps while gathering the IRT and communicating the situation and updating on the incident's steps taken thus far, as well as any other pertinent information.
3. During that same time period, use data capture tools to capture all traffic, 24x7, on even the fastest links.
4. Ensure network recording and store all packets for post-incident, or forensic analysis
5. Force a change of password for all users, including administrators, disable accounts, if necessary, to ensure no one can access sensitive data with already know credentials.

Contact the relevant parties to inform of the incident, including any necessary 3rd parties that specialize in forensics and data breaches to determine the next steps.

7.4.2 Malware / Viruses

During a malware incident, there are a few steps to take to limit exposure:

1. Disconnect devices identified with malware from the network immediately.
2. Examine the malware to identify the type (e.g., rootkit, ransomware, etc.) and establish how it infected the device. This will help the company to understand how to remove it from the device.
3. Once the malware has been removed a full system scan must be performed using the most up-to-date signatures available; to verify it has been removed from the device.
4. If the malware cannot be removed from the device (as is often the case with rootkits) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images, you must verify that the back-up media/images are not infected by the malware.
5. Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attacks.

7.4.3 Unauthorized / Tampered Device Found

When a device is found on the network that is unauthorized, having an updated device list will aid in identifying any rogue devices on the network, if one is found these are the steps to follow:

1. Stop using unauthorized/tampered devices
2. Report the unauthorized/tampered device to the IRT as soon as possible
3. Follow your IRT advice to ensure the security of the devices and carefully inspect and confirm the integrity of your remaining devices, deploy replacement devices, if needed.
4. Investigate the incident and carefully investigate the unauthorized/tampered devices and follow up with any appropriate parties (as needed).

7.4.4 Unauthorized Access

If unauthorized access is detected, or reported by staff, these must be recorded as a security incident. The next steps to take during the process:

1. IRT will investigate to identify the location of the unauthorized access.
2. IRT will investigate as to whether authorized access is being used for a legitimate business purpose/need. If a legitimate business reason is identified, then this access must be reviewed and go through the correct management approval process. This is to make sure that the business justification and access is securely configured (change default passwords and settings, enable strong authentication and encryption).
3. All other unauthorized access must be located, shut down, and removed. This access will be documented in the incident response form provided in the appendix.

7.4.5 Loss / Stolen Equipment

Devices covered under this policy are wholly owned by NEMR, not personal devices used during work hours. If a device is lost or stolen follow these steps:

1. The theft or loss of an asset, such as a PC, laptop or mobile device, must be reported immediately to a member of the IRT and local law enforcement (if applicable). This includes losses/thefts outside of business hours.
2. If the device that is lost or stolen contained sensitive or payment card data, and the device is not encrypted, IRT will complete an analysis of the sensitivity, type, and volume of data stolen, including any potentially exposed payment card numbers.
3. Where possible, use available technology/software to lock down/disable lost or stolen mobile devices (smartphones, tablets, laptops, etc.) and initiate a remote wipe. Evidence should be captured to confirm this was successfully completed.

7.4.6 Social Engineering

Social engineering can take many forms: phone calls, emails, on-site visits, text messages or social media connections. During a social engineering attempt, nefarious characters attempt to entice employees to give up confidential data or to gain access to the network by tricking a user into clicking or installing some sort of malware or exploit. Steps to take if you are the victim of social engineering are:

Contact the IRC or IRT members to inform them of the incident.

1. Document as much as possible, if it is an email document what links were clicked on and what information was entered if it was a phone call or another type of social engineering, as much information as possible like time, date, what/who was asked about and description of the person or caller.
2. Do not forward the email to others, instead, isolate the device from the network, until the device has been cleared for use on the network from the IRT.
3. Change any passwords associated with the account that was socially engineered.
4. Alert any other pertinent employees/parties to the social engineer or the attempt made at it and communicate the steps taken and what to look for from the incident.

7.4.7 Non-Compliance of Security Policies

This section covers incidents resulting from deliberate or accidental actions that are in breach of your security policy, and which put sensitive and payment card data at risk. This includes any systems or data misuse, unauthorized exposure of data to external parties, unauthorized changes to systems or data.

1. IRT/Security officers will engage with the relevant business area to establish an audit trail of events and actions. They will determine who is involved in the policy violation and the extent of the violation.
2. IRT/Security officers and/or line managers will notify General Manager of the incident.
3. IRT/Security officers and/or line managers will liaise with General Manager to determine whether disciplinary action is needed.
4. IRT/Security officers and/or line managers will undertake an assessment of the impact and provide advice and guidance to the business area to prevent reoccurrence, for example, re-training of staff.

7.4.8 Natural Disasters

Like various cyber-attacks, NEMR is aware that natural disasters prone to the geographic area may also cause harm to NEMR's assets. Guidelines have been made to respond to these situations in a safe and efficient manner, prioritizing human safety above all else.

NEMR will outline its process for fire, tornado, flooding, and any other disaster it sees fit. Topics to include are the location of employees, roll call procedures, and response to events.

7.4.8.1 Fire

1. Upon the discovery of a fire, call 911.
2. If the fire is small enough, use the nearest fire extinguisher to extinguish (THIS SHOULD ONLY BE DONE IF THE FIRE CAN BE SURPRESSED QUICKLY AND SAFELY).
3. If the fire grows too large to safely extinguish alone, enclose the fire by shutting doors and contact the fire department (911) immediately.
4. Alert remaining staff of the incident and evacuate the building.

5. Meet with the fire department as they arrive and inform them of the situation.

7.4.8.2 Tornado

1. As soon as a tornado siren is heard, employees should head to the Vault in the office.
2. After it is safe to leave the shelter area a roll call will be conducted, and any injuries will be addressed immediately.
3. An investigation will be conducted to locate all unaccounted-for employees and guests that were present (The physical sign-in sheet will be utilized for this task if still intact).
4. The IR/DR Team will be deployed to identify any devices that have been lost or damaged and will prioritize replacing critical systems and data.

7.4.8.3 Flooding

1. All staff members will be alerted and evacuated to higher grounds. Upon arrival a head count will be conducted.
2. If time allows, the IR/DR Team will procure any critical devices or backup their data. Any physical backups stored onsite will be removed. If this cannot be done in a safe manner the team is to abandon these tasks and evacuate to a remote location or higher grounds with the remaining staff.
3. Depending on the length of the flood, employees will relocate to their home to continue operations.
4. Once able to safely return to the office efforts will be made to restore the building (recovering critical systems, drying out wet areas).

7.4.8.4 Severe Weather

1. NEMR Management will be responsible for communicating with employees whether it is safe to travel to and from the office. The situation may change as the weather worsens. Department managers will communicate these updates to all staff members.
2. Before conditions worsen, appliances and precautions will be tested to ensure they are ready for a severe storm. Staff designated by the Plant Manager will test heaters, thermostats, and lighting systems. An assigned employee will check fuel lines, refill propane as needed and verify all smoke detectors and carbon monoxide detectors are working properly.
3. Plant Manager will inspect areas of the building that may be negatively impacted by cold temperatures (roof/attics with leaks, equipment temperature, etc.)

7.5 Post-Incident Activity Phase

The Post-Incident Activity phase provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The IRT will hold a "lessons learned" meeting within one month after the occurrence of any type of security incident. The meeting will assist in the creation of a follow-up report on the incident. This report provides a reference that can be used to assist in handling similar incidents. Creating a formal chronology of events is important for legal reasons, as it creates a monetary estimate of the amount of damage the incident caused in terms of any loss of software and files, hardware damage, and staffing costs (including restoring services). This estimate may become the basis for subsequent prosecution activity by entities such as the U.S. Attorney General's office. The follow-up reports will be reviewed by the Board and kept for a period of 5 years, as specified by NEMR IRT.

Incident Response Reporting will document all critical information about the situation. The impact of each incident cannot be known at the beginning of, or during the event. Therefore, documentation will be kept pertaining to all security related issues. Documentation of events is preferred to be handwritten to ensure they haven't been tampered with and will be stored in the vault in the main office.

Information to be documented includes:

- Time and Date of the security incident
- Nature and size of the scope
- Description of information exposed, deleted, or altered
- Networks, systems, customers, or individuals affected by the incident.

Questions to be asked during review include:

a. What changes need to be made to security?
b. How should employees be trained differently?
c. What weakness did the breach exploit?
d. How will you ensure a similar breach doesn't happen again?

7.6 Testing & Maintenance

NEMR's IRT understands the success of an IRP can only be proven by performing annual testing or by responding to an actual computer security incident. Documentation and gathering of information during Incident Response, both actual and fictitious, will provide insight on how to improve the NEMR IRP. Annual Round table discussions and scenarios will be used to help prepare management in the event of an incident. All Incident Response reports, and documentation shall be subjected to review by the NEMR Board of Directors as well as an independent auditor. The IRP will be updated annually to reflect changes in the telecom institution. The annual update will also respond to recommendations generated in the Post-Incident Activity phase as well as by the Board review.

According to PCI standards NEMR will conduct quarterly penetration and vulnerability scanning on all PCI networks. This test will be conducted by qualified internal or external parties of the organization. For all external scans, an Approved Scanning Vendor (ASV) will be utilized. Along with all results from the ASV being remediated until NEMR passes the quarterly test. Furthermore, vulnerability testing will be conducted after any major network changes have been made or upon the release of any pertinent zero-day vulnerabilities that affect NEMR resources.

7.7 Third-Party Contact Information

Company Name	Primary Contact	Phone Number	Email
Chariton Valley	Ryan Johnson	660-395-9657	rjohnson@charitonvalley.com
BlueBird Networks	NOC	877-766-2662	noc@bluebirdnetwork.com
Innovative Systems	Jim Reyne	605-995-6120	jimr@innovsys.com
Vantage Point	Gavin Davis	605-995-1794	Gaven.davis@vantagepnt.com

8 Backup Procedures

8.1 Purpose

In today's day and age, data loss can happen at any time for a number of reasons. Whatever the reason, NEMR is committed to operating its systems with as much uptime as possible. Providing service for our customers is our number one priority. Backups of all critical systems will be conducted where possible. SQL databases as well as all customer databases are backed up allowing for ease of recovery assists in the incident response process. These backups are done locally and through Azure. This section will outline the frequency, length kept, location, and process of conducting NEMR's backups.

8.2 Backup Process

NEMR uses Elation software to assist with its backup process. All network data is backed up on a redundant server. Data is also replicated at a secondary data center at Innovative Systems. Daily snapshots are taken to help prevent ransomware attacks. Data to the secondary data center is conducted daily, weekly, and monthly. Daily backups of network data are conducted.

Data is locally retained for 6 months.

Backups will be stored in a way that doesn't allow them to be overwritten or modified after the completion of the backup. To provide a safe and secure environment for them.

8.2.1 Disaster Recovery Site

NEMR will utilize the Unionville CO office as its disaster recovery site in the event the primary location is unavailable. This location has the capacity to support enough employees and infrastructure to restore crucial data in the event of an emergency. The Network Manager stationed at the Unionville office is responsible for maintaining this equipment. The Network Manager will also take points on restoring the data in event other staff members are unable to access these systems.

8.3 Data Privacy

Data is only collected on an as needed for the business use case and is only used for the sole purpose that was designated in the scope of the engagement. Any client data acquired is maintained, protected, and used only by NEMR employees and NEMR designated parties that meet strict guidelines and policies designed to protect that data. Data covered under this policy include any data acquired and maintained through websites, domains, information portals, registries, other online resources, and acquired from clients or other entities on behalf of clients that also meet these terms and conditions. Any links on websites or other public-facing devices that provide and maintain third-party links or databases are not covered under this policy and are not under NEMR control or maintained by NEMR.

9 Form Appendix

9.1 Onboarding/Offboarding Forms

NEMR On-boarding Form						
Employee Name:			**Employee Manager:**			
The top section of the form is completed by the manager requesting the new employee. The bottom section is completed by the IT/IS officer. The change request must be approved before it can be impletemented.						
Start Date:			**Date Requested:** *The date that the request form was completed.*			
Job Title:						
Job Location:						
Work Schedule:						
Orientation Processing						
Drug Test Complete Date			**Physical Complete Date**			
HR/Accounting	**Payroll Setup (I-9, W-4)**		**Insurance**		**Expense Reimbursement Training**	
HR Signature:						
Marketing	**Photo of Employee and/or consent form**				**Employee background write-up**	
Marketing Signature:						
CPNI	**CPNI/Red Flags Training Completed**		**Broadband Labels Training Completed**			
CPNI Trainer Signature:						
IT Access Given (Enter a "Y" or "N" in the boxes)						
User Account Created (M: Created)			Calix Cloud Setup			
Laptop Assigned			Elation Reach Access			
Ipad Assigned			Elation Tech Access			
Door Access and FOB Assignment			Elation Relay Access			
Time Clock Setup (Accounting)			Elation Mapping Access			
ISPN Help Desk Account Created			Elation/Elation + Access			
Bomgar Account Created			Printer Setup			
Email Address Created			Elation Financial Access			
Duo Setup			Slack Setup			
Intelliquent Account Created			Desk Phone Setup			
KnowBe4 Account and Training Setup			Company & Cybersecurity Policy (Intranet-Marketing)			
Technician Inventory Warehouse Setup (Accounting)			AP Max			
IT/Cyber Signature:						
Follow-up Needed: Yes or No						
Manager Signature:						
GM Signature:						

NEMR Off-boarding Form

Employee Name:	**Employee Manager:**
The top section of the form is completed by the manager requesting the new employee. The bottom section is completed by the IT/IS officer. The change request must be approved before it can be impletemented.	
Termination Date:	**Date Requested:** *The date that the request form was completed.*
Job Title:	

Off-boarding Process						
HR/Accounting	**Finalize Last Checks**		**Insurance**			
HR Signature:						

Access/Permissions Revoked			
User Account (M:) Deactivated		Calix Cloud Access Deactivated	
Laptop Returned		Elation Reach Access Deactivated	
Ipad Returned		Elation Tech Access Deactivated	
Door Access and FOB Deactivated/Keys returned		Elation Relay Access Deactivated	
Time Clock Removed - Only after last pay period		Elation Mapping Access Deactivated	
ISPN Help Desk Account Removed		Elation/Elation + Access Deactivated	
Email Address Removed		Elation Financial Access Deactivated	
Duo Setup Deleted		Slack Access Removed	
KnowBe4 Account Deleted		Send email to Innovative to remove user	
IT/Cyber Signature:			
Follow-up Needed: Yes or No			

Company Property Returned:	List any property to include tools, credit cards, vehicles. List excess on separate sheet of paper.		
1		4	
2		5	
3		6	

Notes:

GM Signature:

9.2 Incident Review Form

Incident Review		
Incident Priority: ☐High ☐Medium ☐Low	**Issue Type:** *Work Stoppage, cyber-attack, system malfunction*	
	Date Occurred: *DD/MM/YYYY*	
	Date Resolved: *DD/MM/YYYY*	
System Information		
Location	**Equipment Name**	**User**
Failure Information		
Failure Description	**Cause**	**Remediation**
Work Order Execution		
Technician	**Work Code**	**Date/Time**
1.	*Assign a unique number to each form*	
2.	*Assign a unique number to each form*	
System Downtime: **Parts Used or Required:** **Notes:**		
Approval		
Technician	**Supervisor**	**Identifier**

10 Summary and Conclusions

Cybersecurity threats are not solely a technical problem of computing and network security. New defenses will emerge to combat old threats, and new tools will advance our understanding of networks. Even as technology grows the essential part that stays the same is the people. As companies add more innovation more openings are available for cyberattacks. Even more prevalent than cyber-attacks are social engineering attacks. Attackers use this style to gain information on employees to get access to your network. Allowing them to stay undetected by searching and understanding your network. The cybersecurity mindset must be understood & taught to all staff to allow for a more robust network security standpoint.

Revision History

Date	Updated by	Approved Date